понентов с полученными при расчете результатами показало полное выполнение эргономических требований.

Для проверки соответствия типового алгоритма работы оператора требованиям инженерной психологии необходимо рассчитать коэффициенты стереотипности Z_H и логической сложности L_H , а затем проверить выполнение условий: $0,25 \le Z_H \le 0,85$ и $L_H \le 0,2$. Для Atten Instruments ADS1022C получили $Z_H = 0,46$ и $L_H = 0,18$. В данном случае корректировку алгоритма работы проводить не нужно.

На основании полученных результатов анализа было разработано экспертное заключение о степени соответствия ПУ контрольно-измерительных приборов требованиям дизайна. Таким образом, полученные результаты показали, что методика может использоваться для определения соответствия параметров ПУ сложных технических устройств требованиям дизайна.

В заключение следует отметить, что предложенный метод является более трудоемким, чем метод экспертных оценок. Однако он позволяет значительно более объективно оценить соответствие параметров приборов требованиям инженерной психологии и эргономики, так как базируется на теоретической базе этих дисциплин [2].

Список использованных источников:

1. Алефиренко, В. М. Инженерно-психологические требования к разрабатываемым интерфейсам программных средств / В. М. Алефиренко, С. М. Боровиков // Международная научно-техническая конференция, посвященная 45-летию БГУИР : тезисы докладов междунар. науч.-техн. конф., Минск, 19 марта 2009 г. – Минск : БГУИР, 2009. – С. 106, 107.

2. Основы инженерной психологии: учебник для техн. вузов / под ред. Б. Ф. Ломова. – М.: Высш. шк., 1986. – 448 с.

МОДЕЛИРОВАНИЕ УГРОЗ БЕЗОПАСНОСТИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Дубочинский Р.С

Пачинин В. И. - канд. техн. наук, доцент

Целью исследования, является разработка комплекса мер по улучшению системы защиты информации организации на основе выделенных типов угроз и определение приоритетных направлений ее развития на основе анализа надежности полученной системы защиты.

Для того, чтобы оценить риск информации, необходимо проанализировать все угрозы, действующие на информационную систему, и уязвимости, через которые возможна реализация угроз. Исходя из введенных владельцем информационной системы данных, можно построить модель угроз и уязвимостей, актуальных для информационной системы компании.

На первом этапе рассчитываем уровень угрозы по уязвимости (Th) на основе критичности и вероятности реализации у грозы через данную уязвимость. Уровень угрозы показывает, насколько критичным является воздействие данной угрозы на ресурс с учетом вероятности ее реализации:

$$\mathrm{Th}_{\mathrm{c,I,a}} = \frac{\mathrm{ER}_{\mathrm{c,i,a}}}{100} \times \frac{\mathrm{P(V)}_{\mathrm{c,i,a}}}{100};$$

Чтобы рассчитать уровень угрозы по всем уязвимостям (CTh), через которые возможна реализация данной угрозы на ресурсе, просуммируем полученные уровни угроз через конкретные уязвимости. Аналогично рассчитываем общий уровень угроз по ресурсу (CThR), учитывая все угрозы, действующие на ресурс:

$$\mathrm{CTh} = 1 - \prod_{\mathrm{i=1}}^{\mathrm{n}} (1 - \mathrm{Th});$$

$$\mathrm{CThR} = 1 - \prod_{\mathrm{1=1}}^{\mathrm{n}} (1 - \mathrm{CTh});$$

Риск по ресурсу R рассчитываем по формуле:

$$\mathrm{R} = \mathrm{CThR} \times \mathrm{D};$$

D – критичность ресурса и задается в деньгах или уровнях.

Для расчета эффективности введенной контрмеры необходимо пройти последовательно по всему алгоритму с учетом заданной контрмеры. Т.е. на выходе мы получим значение двух рисков – риска без учета контрмеры ($\mathrm{R_{old}}$) и риск с учетом заданной контрмеры ($\mathrm{R_{new}}$) или с учетом того, что уязвимость закрыта. Эффективность введения контрмеры (E) рассчитываем по формуле:

$$E = \frac{R_{old} - R_{new}}{R_{old}};$$

В результате работы алгоритма мы получим:
- риск реализации по всем угрозам для информационной системы;
- риск реализации по всем угрозам после задания контрмер;
- эффективность контрмеры;
- эффективность комплекса контрмер.

Список использованных источников:

1. Бармен Скотт. Разработка правил информационной безопасности. − М.: Вильямс, 2002. − 208с.

2. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. − М.: ДМК Пресс, 2008. − 544 с.

3. Петренко С. А. Управление информационными рисками. − М.: Компания АйТи; ДМК Пресс, 2004. − 384с.

СИСТЕМА ЗАЩИТЫ ПОМЕЩЕНИЯ ФИРМЫ (КАБИНЕТ ДИРЕКТОРА) ОТ УТЕЧКИ ИНФОРМАЦИИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Высоцкий В.Н.

Алефиренко В.М. – канд. техн. наук, доцент

В работе были рассмотрены и проанализированы каналы утечки информации из кабинета директора, методы и технические устройства её съема, способы и технические средства защиты информации. В результате была разработана система защиты помещения фирмы (кабинета директора) от утечки информации.

Проблема безопасности информации всегда волновала общество. Сегодня она заключается в том, что от качества мер защиты напрямую зависит экономическая безопасность организации.

В качестве объекта защиты был выбран кабинет директора филиала ОАО «АСБ Беларусбанк» на улице Сурганова. Кабинет директора расположен на третьем (последнем) этаже. Вход в него организован через приемную. Защищаемое помещение также граничит с коридором и кабинетом первого заместителя директора. Этажом ниже расположен кабинет отдела инвестиций и корпоративного финансирования. План защищаемого помещения представлен на рисунке 1.

Рисунок 1 – План защищаемого помещения

Помещение рассматривалось с учетом: характеристик ограждающих конструкций (стен, пола, потолка, двери, окон), предметов мебели и интерьера (столы, кресла, шкаф, сейф, доска-экран, картина, комнатные растения), радиоэлектронных средств и электрических приборов (компьютер, телефоны, видеодвойка, вентилятор, настольная лампа, настенные часы), средств коммуникаций (электропроводка, телефонные линии, кабель локальной вычислительной сети, шлейф пожарной сигнализации). В результате исследования были определены каналы утечки информации, перечень угроз и уязвимости объекта. Самые актуальные угрозы приведены ниже.

Наиболее вероятен съем речевой и/или видовой информации при применении миниатюрных фотоаппаратов, видеокамер, диктофонов, закладных аудио записывающих устройств. Их преимущество определяется небольшими размерами, широкими возможностями для маскировки, невысокой стоимостью, возможностью